Concepts and Applications of Composable FORCEnet

JEFF WATERS[1], MICHAEL STELMACH[2], and MARION CERUTI, [3] Ph.D.
Space and Naval Warfare Systems Center, San Diego (SSC-SD)
Code 246201,[1] Code 2841,[2] Code 246206,[3]
53560 Hull Street, San Diego, CA 92152-5001, USA
waters@spawar.navy.mil, stelmach@spawar.navy.mil, marion.ceruti@navy.mil

Abstract: - This paper describes key concepts and applications of composable FORCEnet, which is the US Navy's operational construct architectural framework for naval warfare in the information age. It describes the concepts and architecture, in several categories: 1) systems and general software engineering; 2) networks; 3) intelligent software; and 4) network security. The engineering approach to implement FORCEnet is an example of rapid prototyping in which the requirements of the users reviewed periodically and frequently with considerable user input. Examples of applications of composable FORCEnet include the KWeb, which is a knowledge- and web-based system designed to present the common operating picture to all users. Another example of composable FORCEnet is the Knowledge Management for Distributed Tracking (KMDT), which allows sensor analysts and commanders on ships to access sensor information collected on other ships and shore-based sensor stations, using intelligent-agent and web technology. Composable FORCEnet is designed to capture and implement changes in user requirements. It strongly supports the development of relevant and useful systems with up-to-date technology that will be responsive to the users' rapidly changing needs.

Key-words: - FORCEnet, industrial applications, management of distributed computer resources, security, software engineering

1 Introduction

This work describes the key concepts of Composable FORCEnet (CFn), which is the U.S. Navy's operational construct and architectural framework for naval warfare in the information age [3], [5]. The goal of FORCEnet is to integrate warriors, sensors, command and control, platforms, and weapons into a networked, distributed combat force [5], which is illustrated in Fig. 1. The central theme of information management in future Naval and joint commands includes the development and implementation of a composable architecture based on FORCEnet concepts. Thus, the major contribution of FORCE-net is that war fighters in surface ships, aircraft and submarines, as well as those on shore-based stations no longer have to rely on only the sensor information available to them on in their local area.

With FORCEnet, any information at any site on the network can be made available at the appropriate level of security. Often this information is critical to decisions making and has an enabling effect in reducing the uncertainty that is characteristic of the battle space.

Therefore, an on-going evolution and implementation of the CFn concepts is part of the process of continuous improvement of security and command centers. Each concept of CFn is included in one or more of the following four concept categories: 1) systems and general software engineering; 2) networks; 3) intelligent software; and 4) security, which are covered in sections 2 through 5 respectively. Section 6 describes applications of composable FORCEnet and section 7 concludes the paper.

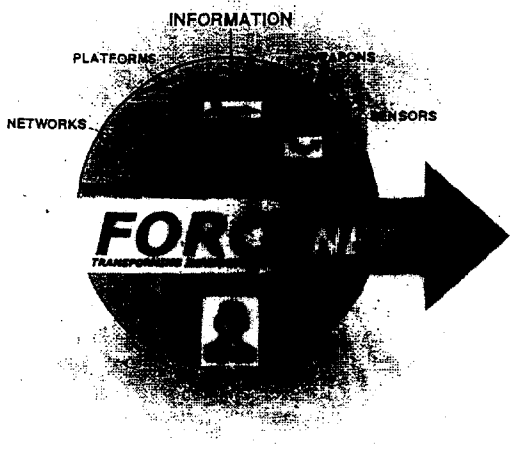

Fig. 1. FORCEnet: Integration of Naval assets via computer networks.

2 Engineering concepts

The fundamental concept is "composability", i.e. to compose the heterogeneous information, systems, and people to meet the mission requirements of the moment. Agile response is the essential. In contrast to the stand-alone architectures, a fluid, agile architecture must be transformed into whatever architecture is needed for the particular mission. The architecture must incorporate new technologies and systems. It must enable the operator or field agent to see the "big" picture and to contribute to it. The CFn architecture is designed to meet these needs. The result is a revolution in both the sharing and the protection of information.

War fighters must have the capability to obtain the information they need when they need it, to analyze and share that information with various people across various systems, networks, and organizations. They must be able to form new systems and teams from these components to fight the battle of the moment. All of the concepts discussed here support this most fundamental and highest-level concept. Currently, the war fighter must expend valuable time and effort to create this unified command-and-control environment. War fighters carry information from one system or network to another and pass information through less-than-ideal means, usually verbally, without shared views or interoperable systems. The information systems of the future must hold all components together, freeing the war fighter to perform higher-level functions, such as decision making. Composability provides this architecture.

Spiral development is another important engineering concept. CFn represents an integration process that includes stages, such as knowledge engineering, mock prototype development, usability testing, prototype development, data-source wrapping, legacy-system integration, tailored-information views, and decision-support agents applied in a spiral-development process. An instantiation of this spiral process within the FORCEnet framework is the SSIM. The integration process is designed to transfer the CFn concepts and approach into an operational command.

Knowledge engineering determines the roles and tasks of operators, as well as the information flow. The knowledge engineering helps to determine the data sources. The information can be published automatically on an information grid, with appropriate policies and safeguards. Decision-support agents monitor and support the automatic insertion of content. The project team connects these data sources, views, and agents

with the architecture, and builds mock-ups and prototype systems for testing. After the initial setup phase, the integration process spirals frequently across these stages, and within these stages, to fill in all the components, train operators, assist with the development of concept of operations, and hone the architecture to meet the needs of the command. In the end, challenging concepts are brought to life quickly to achieve dramatic impacts in an existing command. The CFn prototype and the resulting changes in operations to improve efficiency of command are readily apparent and measurable.

Decentralization and distribution are key concepts to composable FORCEnet. The decentralized approach is needed to support distributed components and scalability. A centralized, or hub-and-spoke, approach works adequately for limited or specialized applications, but it fails when the information is heterogeneous, voluminous, and needed for an unlimited number of perhaps unknown users and unknown applications. Considerable difficulty is encountered in the following tasks: 1) Assemble all the needed information in one place. 2) Maintain the information consistent with the original data source. 3) Avoid single points of failure, and 4) Add new systems and databases. Soon, one begins to create mirror sites, modularize and distribute the information, and adopt a decentralized approach.

Organizations, people, information, systems, operations, and threats are all distributed over as many dimensions, e.g. various physical locations, time periods, systems, and networks. Information systems of the future must interoperate in a distributed manner. An underlying assumption of this concept, as well as many others described here, is that no single technology or operational solution works for all users, all missions, and all informational needs. Instead, the "best" architecture is the most flexible architecture because it allows for the incorporation of various, diverse technologies as they are developed. Part of the flexibility, is the capability to integrate distributed components. The decentralized, distributed approach offers more flexibility for architecture types, making the degree of centralization an optional variable, rather than a given.

Collaboration is an important component of successful operation of missions across diverse organizations and specialized capabilities. One of the important applications of several of the other concepts discussed here, e.g. distributed, net-centric, decentralized, is how they support and contribute to successful collaboration. Groups need not be collocated, huddled over a single system monitor, to discuss the information presented. Now, over shared views through web-browsers anywhere in the world, from any media-wall to any desktop, users can share common views and information. Intelligent agents also share information and expertise. Collaboration, for both people and agents is a fundamental concept underlying future information systems.

The "peer-to-peer" concept is the notion that any component in the network can be linked to any other component on the network, without having to go through a central server. Generally, peer-to-peer architectures offer advantages in scalability and robustness, because they don't rely on a central server. Peer-to-peer also has advantages in flexibility, because two components that are "smart" enough to interoperate can do so, regardless of the capability, or lack of capability, of the other components or servers. A peer-to-peer, loosely coupled architecture facilitates the implementation of new capabilities quickly, without disturbing existing components and without the delay of modifying centralized resources.

Open-web standards foster composability and interoperability. Although the standards represent common agreement, the goal of the standards process should not be misunderstood to force everyone to agree on everything and use all the same specifications because it would limit individual developments and improvements to the changes that could garner universal agreement. Instead, the goal of the standards process is to provide generic representations of inputs and outputs, i.e. links, between diverse components. For example web standards include XML, HTML, and Web Map Server (WMS), which defines a web-based format for accessing map images to be used by any diverse component. Thus, the goal of the standards is to assist

diverse personnel and programs to interoperate, not to limit or constrict them.

"Publish and subscribe" is a concept for distributing one-to-many information, i.e. where one component has information that many clients want. This scheme arises often in information systems, for example where a data source provides information such as tracks or security reports that many other programs need. Publish-subscribe models can be quite flexible. For example, subscribers can find publishers easily, subscribers can come and go as needed, and clients can subscribe to only the portion of the information they need, which is convenient and helps to control bandwidth requirements. The publish-subscribe architecture 1) provides loose coupling between information producers and consumers 2) efficiently includes new subscribers without changes to the architecture, and 3) supports the concepts of modular, distributed, composable components.

Data-source wrapping is the task of designing an open standard, XML schema, definition of the XML tags and data types for a given data source. Rather than the proprietary representation of data often used in legacy systems, the transformation project's approach begins by wrapping data in a reusable and adaptable form. Open standards enable future and currently unknown systems to be interoperable.

Information pedigree is critically important to assess information relevance, reliability, and credibility. Each user in the chain, from the originator to the final decision maker, must assess the confidence of the information. Decision makers must be able to have confidence in the timeliness, accuracy, and implications of information. Data elements may be linked to some originating information or they may be created based on the original information, thus form a chain of dependence. A later reassessment that weakens or destroys the confidence in some particular information may have ripple effects throughout this chain. Data mark-up must incorporate these metadata features. Agents that analyze the information must use appropriate algorithms to assess the confidence. Fuzzy-logic techniques may provide solutions for maintaining the integrity of the confidence, thus avoiding hard-coded thresholds.

3 Intelligent Software Concepts

Agent technology has been used in fleet experimentation to acquire data, monitor information, assemble results, and alert operators [1]. Operators in security centers need autonomous intelligent agents that can subscribe to information and be tailored to screen automatically for reports that match specified patterns that indicate important activity. Such capability is vital to allow the time to make relevant decisions. Agents also can apply rules, alert operators and collect filter, and assemble information automatically.

The agents themselves interoperate in an environment that is a model for composable concepts. Each agent is a distributed, autonomous program, loosely coupled to other agents via publication and subscription of marked-up data and a peer-to-peer text messaging system with directory services to find each other based on attributes. The agent environment is scalable, with multiple machines and distributed lookup services participating. Software agents can provide better support for dynamic logic and better protection for data, thus enabling the "information-rights management" recommended as a major step forward for security and control of information.

Operators will want to query for information any minute of the day and will not always have every possible contingency in mind. An operator needs the capability to ask a question that can be incorporated the agent's daily tasking. Automatic monitoring and alerting allows fewer operators to do more with less.

An ontology is a set of defined terms representing objects or concepts in a domain, and their relationships - a formal representation of knowledge. Gruber defines it as a "specification of a conceptualization" upon which every knowledge base, knowledge-based system, or knowledge-level agent is committed explicitly or implicitly [6]. Ontologies can contain entities, classes, and instances (the noun ontology) as well as concepts that represent actions (the verb ontology). In knowledge-based systems, an on-

tology specifies the entities that exist and the truths that persist about them [2].

The inference engine operates on the knowledge base and data sources to draw conclusions about the state of the system. Ontologies and inference engines are key concepts to enabling an information system of the future where intelligent agents can assist human operators [2].

Whereas ontologies represent knowledge about persistent concepts, business logic is more dynamic, incorporating rules that are valid only for a particular time, a particular area, or a particular mission. Inference engines can process these rules against the current known facts and inferences drawn from the ontology to modify the knowledge base or to take external actions. The goal is to combine both the long-term and short-term rules and inference engines to enable intelligent agents to monitor information and recommend appropriate actions.

The eXtensible Markup Language (XML) is one of the most widely accepted and supported open standards. XML and the associated XML Schema together represent a data format that makes information reuse extremely efficient [4]. XML enables information to be stored in a format that is understood by developers world wide. It is supported by parsers, and various display and editing tools. New standards for mark up, such as Web Ontology Language (OWL), with even more power for representing meaning and relationships, are based on these original standards. The revolution in mark up is a driving force underlying the effort to allow people and intelligent agents to read internet web pages.

4 Network Concepts

The goal of a "virtual" information grid is to enable all of the benefits of a "physical" information grid, without its limitations, i.e. that all users be physically co-located on the same network using the same systems on the same centralized server. Any user or program should be able to "plug into" the grid and have efficient, seamless access to any and all information needed to perform a mission. One should be able to perform the following actions: 1) Find information producers. 2) Subscribe the information. 3) Receive "marked up" information for reuse. 4) Produce and distribute information in a reusable format. 5) View, annotate, and use the information for collaboration, measuring confidence and determining pedigree when needed. Many other concepts, such as data markup and network centricity, enable a scalable virtual information grid.

To realize CFn, horizontal integration must be implemented across organizations and networks operated at different security levels. The virtual information grid must support the seamless sharing of information across organizations, departments, public and private entities. This includes users who support diverse domains, including research, development, experimentation, and operations. Information must be shared automatically and rapidly across traditional physical and cultural barriers. Primary among these traditional barriers is the classification of entire networks. An organization may find itself on a different network from that of its customers.

The users of the information grid will continue to have problems with bandwidth. The architecture must accommodate those with limited bandwidth. To help address these issues, a filter can significantly limit the amount of information transferred during a publish/subscribe event. Another way is to use intelligent agents is to monitor bandwidth traffic and tailor output based on throughput. Agents can reduce bandwidth requirements by sending only processed data over the network [1].

Network-centric warfare implies that web-based information valuable to the war fighter is available from sensors and other sources that do not reside on a single ship or aircraft. Successful military operations must be based on information, systems, and collaboration, using a network of distributed components. (See, for example [5]). This "network-centric" concept offers many advantages. One of the most significant is the ability to have "virtual" presence, where the components can work together as though physically nearby, even when they may be widely distributed. Another significant advantage is the use of open standards developed for the Internet for communications (e.g. TCP/IP), for information presentation (e.g. HTML), and for image formatting (e.g. jpg, gif), to name a few.

These concepts described above can enable a "self-aware" network that can apply rules to information sources automatically without specific tasking by human operators. The concept of a network that runs automatically without waiting for operator queries, is important for scalability because the number of operators is insufficient to scale to voluminous data sources. Such an intelligent network also can increase the speed of decision making by reducing the query-response time. The network must have marked-up data, ontologies, and rules with action agents to facilitate the propagation of new information and provide alerts and recommendations to decision makers. Operators should function at a higher level using pedigree, confidence, and drill-down capabilities to analyze the information presented and make decisions.

5 Security Concepts

The "need to share" information is emerging in the security community as the new paradigm for information systems. This is a radical departure from the traditional security "need-to-know" mind set. Today, operators receive few incentives encouraging them to share information. They are encouraged to keep their information secret and proprietary. Many penalties are associated with improperly releasing information, but traditionally, few or no penalties have been applied for withholding information. The lessons learned from recent tragedies include the identification of this cultural problem. The concepts described in this section emphasize the need to share and yet provide better mechanisms, e.g. information rights management, than those commonly practiced to protect information from inappropriate use.

Strong data protection is another important security concept in composable FORCEnet. Personnel protect data in a combination of classified networks, classified symbols and annotations using detailed and often confusing or contradictory policies and procedures. A better approach, providing both greater sharing and greater protection, is to mark up the data, provide a combined classification-security-permission tagging of data elements, and to use the approach of information-rights management to enforce the security requirements as data are distributed throughout the network. Information-rights management is a practice based on the notion that the architecture could enforce the security.

Therefore, data could be distributed but with restrictions, such as no printing, e-mailing, or copying. No automatic enforcement is inherent today among stand-alone systems and the reliance is on humans to understand and enforce complex security rules. When data are distributed, no mechanism can provide automatic protection against malicious, or innocent but inappropriate, redistribution of data.

Anonymization is a key concept that helps to lower the classification of otherwise classified data and to lower the privacy concerns associated with personal data. Anonymization is achieved when information is broken into two parts, for example classified vs. unclassified or private vs. public data with the classified or private portion made anonymous. For example, often details about the data source raise the classification of a security report. In this case, the data-source information would be extracted from the security report and that information would be made anonymous in the releasable version. Often, identifying information makes personal information private because the aggregate of these data can identify an individual uniquely. The identifying information can be extracted and the formerly private information becomes anonymous. Thus, the information no longer presents the same level of privacy concerns. The linkage to the original information is maintained so that in the future, if the right conditions are satisfied for those with sufficient clearance and need to know, the data source could be revealed.

With agents applying business logic to standard data sources, lower classification reports can be distributed automatically. Private information, such as crew information on a high-interest vessel, could be anonymized automatically and thereby achieve the dual goal of greater information sharing and greater protection of classified or private information. This concept could have an impact that is potentially revolutionary, where information critical to un-

covering a future terrorist plot, but that initially appears quite private, could be collected, automatically anonymized, and used in a terrorist investigation. Only if enough connections are made with this anonymous information, with a review by a third party for sufficient probable cause, could the anonymity be broken.

Authentication is the ability to confirm a user's (or an agent's) identity. Auditing is the recording of actions taken by that user (or agent). Together, authentication and auditing allow an information system to determine the pedigree of information, to include who or what created and modified the information and how; who used, processed, or annotated it; and who distributed it to whom. Information may be used to take important actions with potentially grave consequences. Decision makers must understand how the information that they use was compiled. For drill down and double checks, users at all levels must know the pedigree.

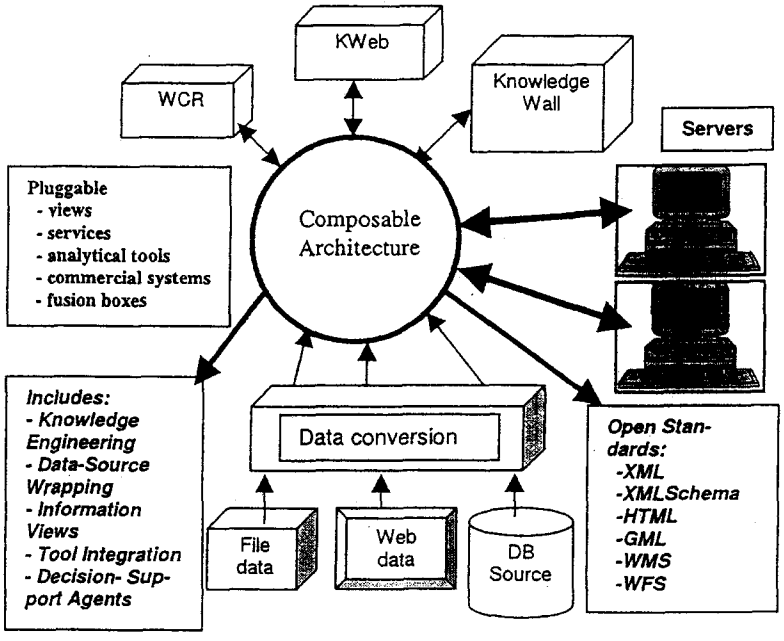

Fig. 2. Virtual integration concept: application of composable FORCEnet [5] and approach to integrate data sources, tools, acquisitions, legacy systems, open standards and warfare-center resources (WCR) from laboratories.

6 Application Examples

To illustrate the concepts of composable FORCE-net, Fig. 2 depicts how information from multiple servers and sources is shared in a modular environment that features "plug and - play" software tools and services. This architecture supports the implementation of FORCEnet-through various projects, such as the Knowledge Web (KWeb) and the Knowledge wall, which includes a large-group display.

The KWeb is installed in a security center and has resulted is a much more efficient integration and utilization of information across the organization.

The second example of the application of composable FORCEnet principles, shown in Figure 3, is a modeling-and-simulation project known as Knowledge Management for Distributed Tracking (KMDT). The focus of KMDT is on network-based level-one (detection, localization, classification) data fusion and threat identification. (See, for example, [2].)

The goal of the KMDT is to allow war fighters to reduce uncertainty by better organizing and using the data collected from existing sensors. To achieve this goal, KMDT will initially integrate technologies that are essential for the design of next-generation tracking systems, including knowledge management techniques, line-of-bearing cross fixing, sensor models, and network-based command and control. The capabilities described in Figure 3 would be difficult or impossible to implement routinely without the FORCEnet

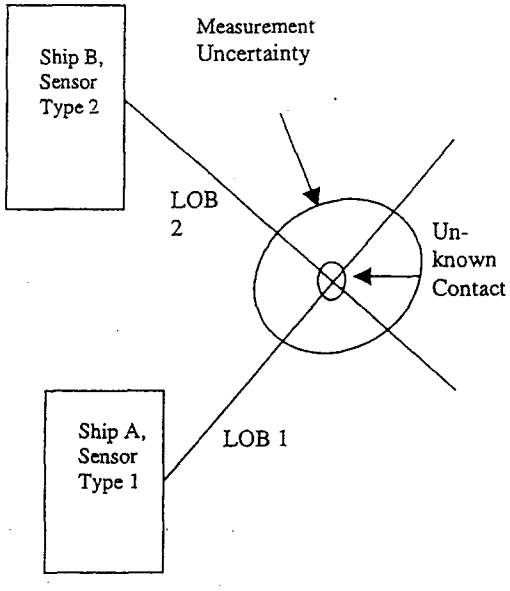

Fig. 3. KMDT detection geometry showing lines of bearing from ships A and B detecting an unknown contact with heterogeneous sensor types 1 and 2.constructs in place.

7 Conclusion

CFn represents the articulation of a vision, a roadmap to the future. The concepts outlined above explain an approach to incorporate new technologies and support new operations.

This will be accomplished through open standards, decentralized peer-to-peer architecture, and through composing flexible, loosely coupled, and modular components. Using the CFn concepts and approach, organizations can work together to share and reuse information and systems, yet retain their capabilities without making rapid changes in their infrastructure.

Acknowledgements

The authors thank the Office of Naval Research for their support of this work and Dr. Scott McGirr of the Space and Naval Warfare Systems Center, San Diego, for helpful discussions and contributions regarding the implementation of FORCEnet. This paper is the work of U.S. Government employees performed in the course of their employment and no copyright subsists therein.

References:

[1] M.G. Ceruti and B.J. Powers, "Intelligent Agents for FORCEnet: Greater Dependability in Network-Centric Warfare," *Supplemental Volume of the Proc. of the IEEE International Conference on Dependable Systems and Networks (DSN 2004)*, pp. 46-47, June 2004.

[2] M.G. Ceruti, "Ontology for Level-One Sensor Fusion and Knowledge Discovery," *Proc. of the 2004 International Knowledge Discovery and Ontology Workshop (KDO-2004)*, 20-24 Sep. 2004.

[3] R.W. Mayo, VADM, USN and J. Nathman, VADM, USN, "Sea Power 21 Series – Part V: ForceNet: Turning Information into Power," *Naval Institute Proceedings*, vol. 129, no. 2, pp. 42-46, Feb. 2003.

[4] J.D. Neushul and M.G. Ceruti, "Sensor Data Access and Integration Using XML Schemas for FORCEnet," *Space and Naval Warfare Systems Center San Diego Biennial Review*, 2005.

[5] V. Clark, ADM, USN, "Sea Power 21 Series – Part I: Projecting Decisive Joint Capabilities," *Naval Institute Proceedings*, vol. 128, no. 10, pp. 32-41, Oct. 2002.

[6] T.R. Gruber, "A Translation Approach to Portable Ontology Specifications," *Knowledge Acquisition*, vol. 5, no. 2, pp. 199-220, 1993.